V159

PCT WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 6 : G06F 1/00 — A1

(11) Internationale Veröffentlichungsnummer: **WO 99/63419**

(43) Internationales Veröffentlichungsdatum: 9. Dezember 1999 (09.12.99)

(21) Internationales Aktenzeichen: PCT/DE99/01461

(22) Internationales Anmeldedatum: 14. Mai 1999 (14.05.99)

(30) Prioritätsdaten:

198 24 163.1	29. Mai 1998 (29.05.98)	DE
198 28 936.7	29. Juni 1998 (29.06.98)	DE

(81) Bestimmungsstaaten: BR, CN, IN, JP, KR, MX, RU, UA, europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Veröffentlicht
Mit internationalem Recherchenbericht.
Vor Ablauf der für Änderungen der Ansprüche zugelassenen Frist; Veröffentlichung wird wiederholt falls Änderungen eintreffen.

(71) Anmelder: SIEMENS AKTIENGESELLSCHAFT [DE/DE]; Wittelsbacherplatz 2, D–80333 München (DE).

(72) Erfinder: SEDLAK, Holger; Neumünster 10A, D–85658 Egmating (DE). SÖHNE, Peter; Holzbauernweg 7, D–85244 Röhrmoos (DE). SMOLA, Michael; Jutastrasse 17, D–80636 München (DE). WALLSTAB, Stefan; Gustav–Heinemann–Ring 55, D–81739 München (DE).

(54) Title: METHOD AND DEVICE FOR PROCESSING DATA

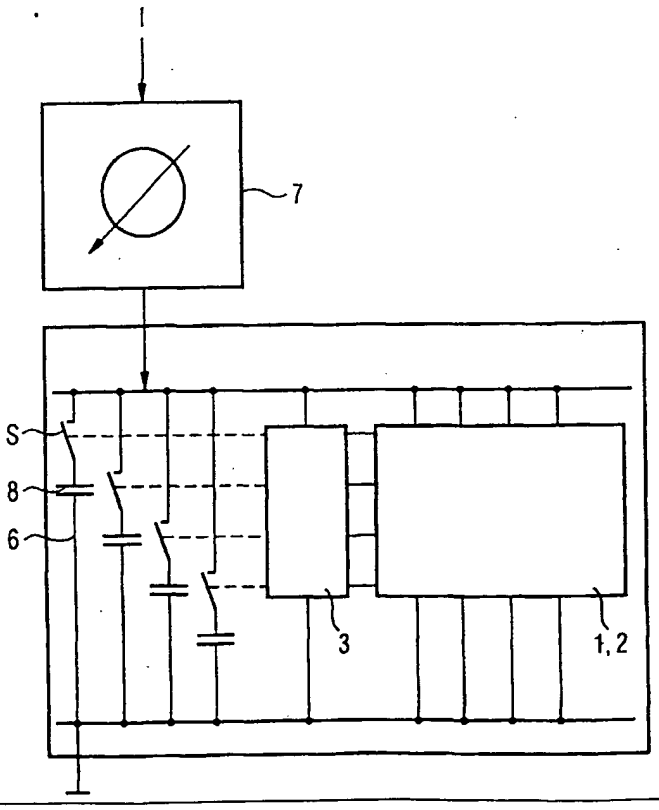
(54) Bezeichnung: VERFAHREN UND VORRICHTUNG ZUM VERARBEITEN VON DATEN

(57) Abstract

The invention relates to a method for encoding and/or decoding data, according to which the data are designated for encoding or decoding in an encoding or decoding step which is chosen from several alternative, equivalent encoding or decoding steps and/or consists of several partial encoding or decoding steps to be processed sequentially. The selected encoding or decoding step is chosen randomly and/or the encoding or decoding steps are modified randomly.

(57) Zusammenfassung

Es ist ein Verfahren zum Verschlüsseln und/oder Entschlüsseln von Daten, bei dem die Daten für ein Verschlüsseln oder Entschlüsseln in einem Verschlüsselungs– oder Entschlüsselungsschritt vorgesehen werden, der aus mehreren alternativen gleichwertigen Verschlüsselungs– oder Entschlüsselungsschritten ausgewählt ist, und/oder aus mehreren sequentiell abzuarbeitenden Verschlüsselungs– oder Entschlüsselungsteilschritten besteht, wobei der ausgewählte Verschlüsselungs– oder Entschlüsselungsschritt zufällig ausgewählt ist und/oder die Verschlüsselungs– oder Entschlüsselungsschritte zufällig verändert sind, vorgesehen.



LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	ES	Spanien	LS	Lesotho	SI	Slowenien
AM	Armenien	FI	Finnland	LT	Litauen	SK	Slowakei
AT	Österreich	FR	Frankreich	LU	Luxemburg	SN	Senegal
AU	Australien	GA	Gabun	LV	Lettland	SZ	Swasiland
AZ	Aserbaidschan	GB	Vereinigtes Königreich	MC	Monaco	TD	Tschad
BA	Bosnien-Herzegowina	GE	Georgien	MD	Republik Moldau	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagaskar	TJ	Tadschikistan
BE	Belgien	GN	Guinea	MK	Die ehemalige jugoslawische Republik Mazedonien	TM	Turkmenistan
BF	Burkina Faso	GR	Griechenland			TR	Türkei
BG	Bulgarien	HU	Ungarn	ML	Mali	TT	Trinidad und Tobago
BJ	Benin	IE	Irland	MN	Mongolei	UA	Ukraine
BR	Brasilien	IL	Israel	MR	Mauretanien	UG	Uganda
BY	Belarus	IS	Island	MW	Malawi	US	Vereinigte Staaten von Amerika
CA	Kanada	IT	Italien	MX	Mexiko		
CF	Zentralafrikanische Republik	JP	Japan	NE	Niger	UZ	Usbekistan
CG	Kongo	KE	Kenia	NL	Niederlande	VN	Vietnam
CH	Schweiz	KG	Kirgisistan	NO	Norwegen	YU	Jugoslawien
CI	Côte d'Ivoire	KP	Demokratische Volksrepublik Korea	NZ	Neuseeland	ZW	Zimbabwe
CM	Kamerun			PL	Polen		
CN	China	KR	Republik Korea	PT	Portugal		
CU	Kuba	KZ	Kasachstan	RO	Rumänien		
CZ	Tschechische Republik	LC	St. Lucia	RU	Russische Föderation		
DE	Deutschland	LI	Liechtenstein	SD	Sudan		
DK	Dänemark	LK	Sri Lanka	SE	Schweden		
EE	Estland	LR	Liberia	SG	Singapur		

Beschreibung

Verfahren und Vorrichtung zum Verarbeiten von Daten

Die Erfindung betrifft ein Verfahren bzw. eine Vorrichtung zum Verarbeiten von Daten. Im Rahmen üblicher Datenverarbeitung werden heutzutage zunehmend Sicherheitsaspekte relevant, da zunehmend versucht wird, unerlaubt Daten aus Datenverarbeitungsanlagen zu erhalten. Um die zu verhindern werden zunehmend kryptographische Verfahren angewandt, bei denen zu schützende Daten verschlüsselt werden. Hierzu wird unter anderem beispielsweise das "Public-Key-Verfahren" verwendet, bei dem jeder Teilnehmer eines Systems ein Schlüsselpaar besitzt, das aus einem geheimen Schlüsselteil und einem öffentlichen Schlüsselteil besteht. Die Sicherheit der Teilnehmer beruht nun darauf, daß der geheime Schlüsselteil Unbefugten nicht bekannt ist. Die Ausführung eines derartigen Verfahrens geschieht häufig in einer besonders gesicherten Komponente, wie beispielsweise einer Chipkarte aber auch in einem einmal in ein Gerät eingesetzten elektronischen Schaltkreis - auch als IC bekannt -, in denen dann das Verfahren selbst realisiert ist. Somit braucht der geheime Teil des Schlüssels diese gesicherte Komponente nicht zu verlassen.

Neuerdings sind jedoch Angriffe bekannt geworden, bei denen versucht wird, den Schlüssel in der gesicherten Komponente auszuspähen. Dies soll beispielsweise durch Messung des Stromverbrauchs der gesicherten Komponente ermöglicht werden. Durch das häufig wiederholte Beobachten des Stromverlaufs und bei dem Bekannt sein wie der Verschlüsselungsvorgang durchgeführt ist, ist es schließlich möglich, Rückschlüsse auf den Schlüssel zu ziehen.

Der Erfindung liegt daher die Aufgabe zugrunde, ein Verfahren zum Verschlüsseln bzw. eine Vorrichtung vorzusehen, bei der eine erhöhte Sicherheit vor dem Ausspähen eines geheimen Schlüsselwortes gegeben ist.

Diese Aufgabe wird erfindungsgemäß mit den Maßnahmen bzw. Mitteln gemäß Patentanspruch 1 bzw. Patentanspruch 3 gelöst.

Dadurch, daß Verschlüsselungs- bzw. Entschlüsselungsverfahren so gesteuert bzw. Operationen begleitend zu diesem Verfahren gesteuert werden, daß sich auch bei einer häufig wiederholten Messung von von außen zugänglichen Parametern, wie beispielsweise dem Stromverbrauch, keine Rückschlüsse auf den verwendeten Schlüssel ziehen lassen.

Weitere vorteilhafte Ausgestaltungen der Erfindung sind in den Unteransprüchen angegeben. Nachfolgend wird die Erfindung unter Bezugnahme auf die Zeichnung anhand von Ausführungsbeispielen erläutert.

Hierbei zeigen:

Fig. 1 ein erstes Ausführungsbeispiel einer erfindungsgemäßen Vorrichtung,

Fig. 2 ein zweites Ausführungsbeispiel einer erfindungsgemäßen Vorrichtung, anhand der auch das erfindungsgemäße Verfahren erläutert wird und

Fig. 3 ein drittes Ausführungsbeispiel

Mit 1, 2 ist eine zu schützende Schaltung, die beispielsweise aus einem Mikrocontroler 2 und einem Rechenwerk 1 besteht, bezeichnet. Der Mikrocontroler 2 steuert dabei das Rechenwerk 1, in dem beispielsweise ein Verschlüsselungsvorgang durchgeführt wird. Dieser zu schützenden Anordnung wird nunmehr ein Strom I zugeführt, der mittels einer Meßeinrichtung 7 detektierbar ist, wodurch Rückschlüsse auf die Vorgänge in der zu schützenden Schaltung 1, 2 gezogen werden sollen. Es ist nunmehr eine zusätzliche Schaltungseinrichtung 6 vorgesehen, die über einen Zufallsgenerator 3 gesteuert wird. Dieser Zufalls-

generator kann beispielsweise als ein Sequenzgenerator in Form eines linear rückgekoppelten Schieberegisters ausgeführt sein, welches mit einem Startwert geladen, eine pseudozufällige Folge - Nullen und Einsen - erzeugt. Hierbei kann der Startwert entweder zufällig erzeugt sein oder von der Steuereinrichtung beispielsweise auf Basis des Schlüsselwortes generiert werden, auch ist eine Kombination beider Möglichkeiten denkbar. Die somit vom Zufallsgenerator erzeugte Sequenz steuert nunmehr Schalter S in der zusätzlichen Schaltungseinrichtung 6, so daß Kondensatoren, die mit den Schaltern S in Reihe liegen, entsprechend der jeweils gerade erzeugten Zufallsfolge geladen werden. Auf diese Weise wird der Stromverbrauch der zu schützenden Schaltung 1, 2 durch die zusätzliche Schaltungseinrichtung 6, nämlich dem Ladestrom der Kondensatoren, verschleiert. Um den Gesamtstromverbrauch dieser Einrichtung zu minimieren, ist es nicht notwendig, daß die zusätzliche Schaltungseinrichtung 6 fortwährend einen Beitrag zum Stromverbrauch liefert. Sie kann vielmehr darauf beschränkt werden, nur in der Zeit während des Verschlüsselns bzw. Entschlüsselns zu arbeiten.

Fig. 2 zeigt ein weiteres erfindungsgemäßes Ausführungsbeispiel. Hierbei liegt das Rechenwerk 1 und die Steuerungseinrichtung 2, der Zufallsgenerator 3 und eine Speichereinrichtung 5 an einem gemeinsamen Bus 4, der von extern mittels einer Schnittstelle 9 zugänglich ist. Über die Schnittstelle 9 werden beispielsweise zu verschlüsselnde bzw. zu entschlüsselnde Daten zugeführt. In der Speichervorrichtung 5 ist ein geheimes Schlüsselwort gespeichert, das gesteuert von der Steuereinrichtung 2 dem Rechenwerk 1 zugeführt wird, um die über die Schnittstelle 9 vom Datenbus zugeführten Daten zu verschlüsseln bzw. zu entschlüsseln. Der Zufallsgenerator 3 erzeugt nunmehr eine Zufallszahl, die der Steuereinrichtung 2 zugeführt wird, die nunmehr auf Grundlage dieser Zufallszahl das Rechenwerk 1 steuert. Hierbei sind nunmehr zwei Möglichkeiten denkbar.

Das Rechenwerk 1 wird auf Grundlage der Zufallszahl durch die Steuereinrichtung 2 so gesteuert, daß der Verschlüsselungs- oder Entschlüsselungsalgorithmus der jeweiligen Zufallszahl entsprechend moduliert wird. Das bedeutet, es erfolgen somit im Verschlüsselungs- bzw. Entschlüsselungsalgorithmus Rechenoperartionen, die ohne abschließende Auswirkung auf die Verschlüsselung bzw. Entschlüsselung, mit zufälligen Werten arbeiten.

Nachfolgend werden Beispiele für die Variationen des Verschlüsselungs- bzw. Entschlüsselungsalgorithmus beschrieben.

Ein bekanntes Verfahren ist das sogenannte RSA-Verfahren. Es arbeitet in der Gruppe teile fremder Restklassen modulo N und setzt die Exponentiationen aus Multiplikationen modulo N zusammen. Die Varianten dieser Protokolle für elliptische Kurven modulo p besitzen aus modularen Additionen und Multiplikationen zusammengesetzte Grundoperationen, sogenannte Additionen und Verdoppelungen in der Punktgruppe der elliptischen Kurven, die ihrerseits zur Exponentiation zusammengesetzt werden. Die dritte große Gruppe besteht aus elliptischen Kurven über endlichen Körpern, deren Elementezahlen eine Primzahlpotenz, die häufig eine Potenz von 2 ist. Diese Strukturen werden gemeinhin als $GF(p^n)$ bezeichnet. Die Basisarithmetik in diesen Körpern kann durchgeführt werden, indem man die Körperelemente als Polynome mit Koeffizienten aus dem Grundkörper GF(p) oder einem geeigneten Zwischenkörper darstellt, die durch Multiplikationen modulo einem festen Körperpolynom miteinander verknüpft sowie koeffizientenweise addiert werden. In diesem Sinne lassen sich Operationen in $GF(p^n)$ bzw. in elliptischen Kurven über diesen Körper als modulare Rechenoperation auffassen. Dabei sind die nachfolgenden drei, dem erfindungsgemäßen Verfahren entsprechende Variationsmöglichkeiten möglich.

a) Der Modul N wird durch r*N ersetzt, wobei r eine von 0 verschiedene Zufallszahl ist. Im $GF(p^n)$-Fall wird das Kör-

perpolynom durch sein Produkt mit einem zufällig gewählten von 0 verschiedenen Polynom ersetzt. Dieser Schritt ist vor Eintritt in die Rechnung oder einem Teilschritt durchzuführen und nachfolgend durch eine Reduktion des Ergebnisses bzw. Teilergebnis modulo N zu kompensieren.

b) Ein Eingangsparameter X einer modularen Rechenoperation wird durch den Wert X + s*N ersetzt, wobei s eine Zufallszahl ist. Dies kann in verschiedenen Rechenschritten durchgeführt werden. Auch eine entsprechende Veränderung mehrerer Eingangsparameter der selben Operation ist möglich.

c) Die Exponenten E werden durch E + t*q ersetzt, wobei t eine Zufallszahl und q die sogenannte Ordnung der Basis der auszuführenden Exponentiation, oder ein geeignetes Vielfaches davon, ist. Potentielle Werte von q lassen sich häufig aus den Systemparametern ableiten. So kann man für die Exponentiation modulo N $q=\varphi(N)$ und für elektrische Kurven q als die Anzahl der Punkte dieser Kurve wählen, wobei häufig noch bessere Wahlmöglichkeiten gegeben sind.

Eine weitere Möglichkeit besteht darin, daß alternative, gleichwertige Verschlüsselungs- bzw. Entschlüsselungsalgorithmen im Rechenwerk 1 durchführbar sind, die gemäß der zugeführten Zufallszahl zufällig ausgewählt werden.

Bei der zuvor beschriebenen Modulation des Verschlüsselungs- bzw. Entschlüsselungsalgorithmus wird nicht nur der Stromverbrauch der Anordnung durch die Zufallszahl verändert, sondern ebenfalls die benötigte Rechenzeit. Auch diese kann als Meßgröße Rückschlüsse auf den Geheimschlüssel geben. Gleiches gilt für die zufallsgesteuerte Auswahl der äquivalenten Rechenoperationen.

Eine dritte Möglichkeit ist darin zu sehen, daß ähnlich dem Ausführungsbeispiel nach Fig. 1 eine zusätzliche Schaltungseinheit 6 vorgesehen ist (gestrichelt dargestellt), die ebenfalls mit der Zuführeinrichtung 4 verbunden ist. Die Steuereinrichtung 2 steuert nunmehr die zusätzliche Schaltungsein-

richtung 6 gemäß einer vom Zufallsgenerator 3 über die Zuführeinrichtung 4 zugeführten Zufallszahl. Eine Anlayse des Stromverbrauchs der dargestellten Gesamtanordnung ist somit nicht durch den Betrieb im Rechenwerk 1 allein bestimmt sondern ebenfalls durch einen zufällig gesteuerten Stromverbrauch der zusätzlichen Schaltungseinheit.

Zusätzlich sei darauf hingewiesen, daß auch die Kombination von Modulation des jeweiligen Algorithmus mit einer zusätzlichen Schaltungseinheit 6 im "Dummy-Betrieb" sinnvoll ist.

Fig. 3 zeigt ein drittes erfindungsgemäßes Ausführungsbeispiel. Hierbei wird der Steuereinrichtung 2, in Form einer CPU über Datenanschluß D Daten zugeführt. Gleichzeitig wird der "Wait-State-Anschluß" WS mit einem Zufallsgenerator 3 verbunden. Dieser Zufallsgenerator 3 erzeugt nunmehr in zufälliger Folge "Einsen" "Nullen". Entsprechend der Programmierung wird nunmehr immer dann wenn eine "1" oder "0" am Eingang anliegt, der Betrieb der CPU gestoppt oder wieder aufgenommen. Dies führt dazu, daß der Betrieb der CPU zwar noch synchron zu einem nicht dargestellten Taktgenerator arbeitet, jedoch keine einheitlichen Verarbeitungszyklen mehr aufweist. Da auf diese Weise kein fester einheitlicher Rahmen mehr vorliegt, sind durch Beobachtung der CPU deren Arbeitsvorgänge nicht mehr ohne weiteres nachvollziehbar und nur sehr erschwert analysierbar. Dies bedeutet, daß die in der CPU abzuarbeitenden Vorgänge "verrauscht" sind. Um die Handhabbarkeit einer solchen Anordnung zu steigern, kann der Zufallsgenerator 3 so programmiert werden, daß festlegbar ist, in welchem zeitlichen Rahmen eine Verarbeitung maximal abläuft. Dies ist unter anderem dafür notwendig, um festzustellen, ob das System insgesamt ausgefallen ist.

Es erscheint besonders sinnvoll eine Anordnung gemäß Fig. 3 mit einer Anordnung gemäß Fig. 1 oder 2 oder mit beiden zu kombinieren um somit beispielsweise die Analyse der Bearbeitung eines Gesamtsystems zu erschweren.

Patentansprüche

1. Datenverarbeitungsverfahren, bei dem in einer Verarbeitungseinheit (1,2) über eine Datenleitung zugeführte Daten verarbeitet werden, ein Zusatzsignal der Verarbeitungseinheit zugeführt wird, und bei dem die Verarbeitung in Abhängigkeit vom Zusatzsignal erfolgt.

2. Datenverarbeitungsverfahren nach Anspruch 1, bei dem das Zusatzsignal von einem Zufallszahlgenerator gesteuert ist.

3. Datenverarbeitungsverfahren nach Anspruch 2, bei dem an einer geeigneten Stelle ein Operand mit einer Zufallszahl beaufschlagt ist und an einer weiteren geeigneten Stelle ein entsprechender Kompensationsoperand mit der gleichen Zufallszahl beaufschlagt ist.

4. Datenverarbeitungsverfahren nach Anspruch 2, bei dem die Verarbeitung der Daten aus mehreren Einzelschritten zusammengesetzt ist, die aus mehreren Alternativen gleichwertigen Einzelschritten ausgewählt sind, und/oder aus mehreren sequentiell abzuarbeitenden veränderbaren Einzelschritten besteht, wobei die Auswahl und/oder die Veränderungauf Grundlage des Zusatzsignals erfolgt.

5. Vorrichtung zum Durchführen des Verfahrens nach Anspruch 1, mit einer Recheneinrichtung (1), der Daten mittels einer Zuführvorrichtung (4) zugeführt werden, und einem Zufallsgenerator (3), und einer Steuervorrichtung (2), die die Recheneinrichtung steuert, wobei ein Ausgangssignal des Zufallsgenerators (3) die Steuereinrichtung (2) und/oder und die Recheneinrichtung (2) beeinflußt.

6. Vorrichtung nach Anspruch 5, bei der mit der Steuereinrichtung (2) eine Hilfsschaltung (6) verbunden ist, die von der Steuereinrichtung (2) auf Basis des von dem Zufallsgenerator (3) zugeführten Ausgangssignal gesteuert wird.

FIG 1

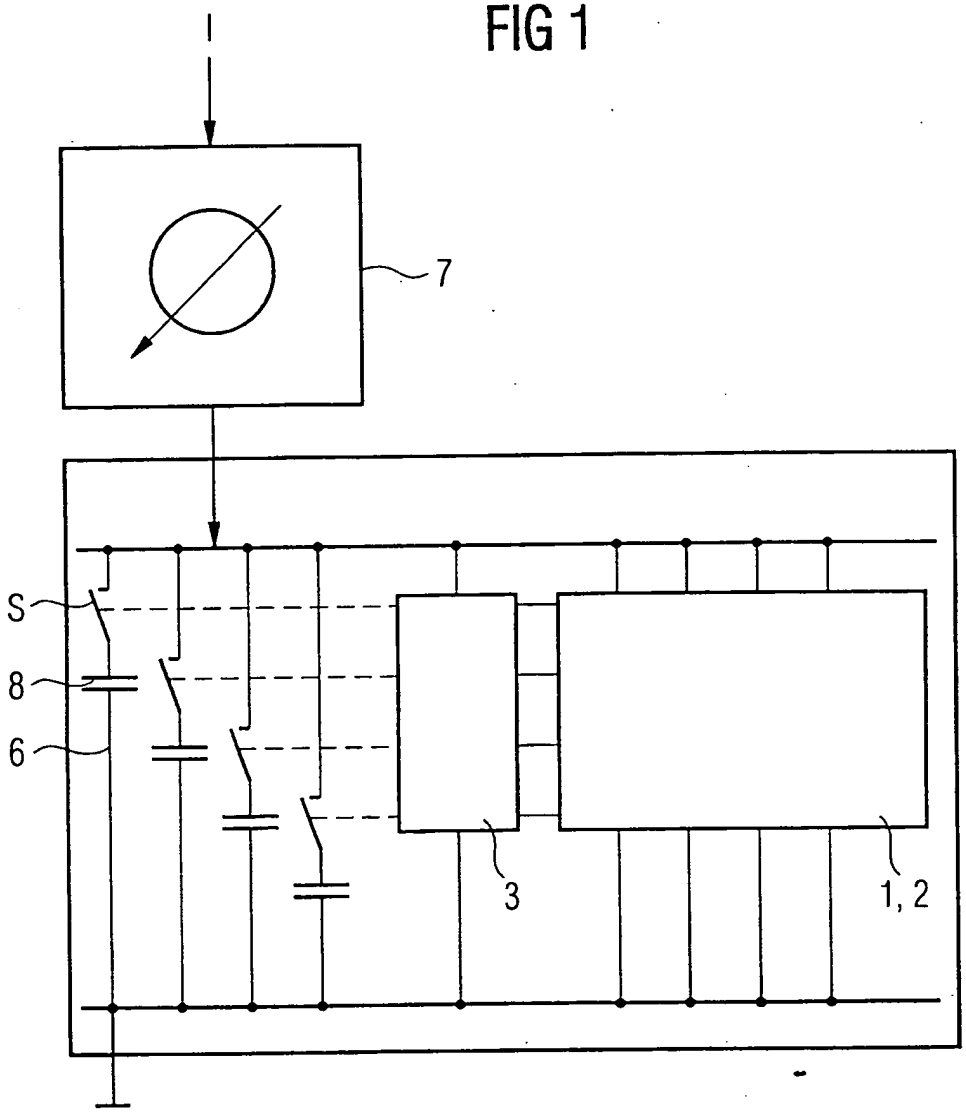


FIG 2

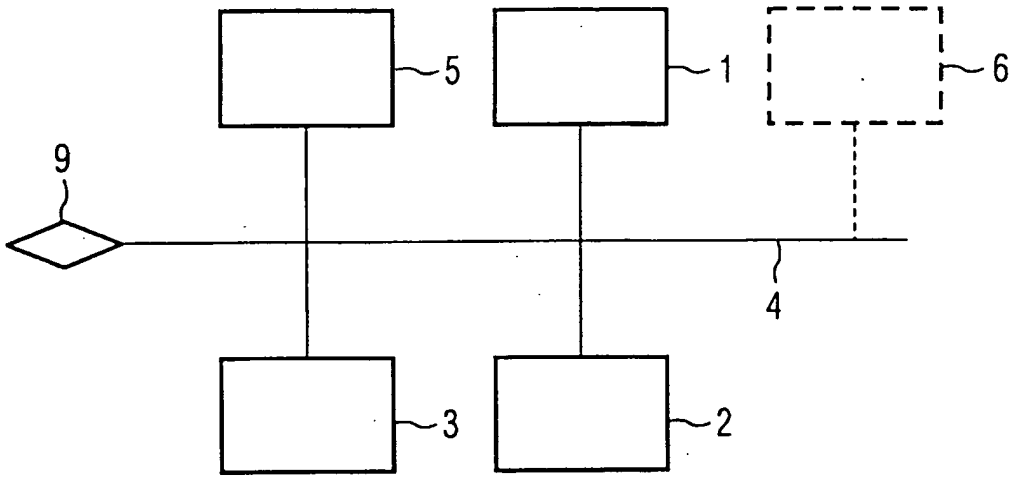
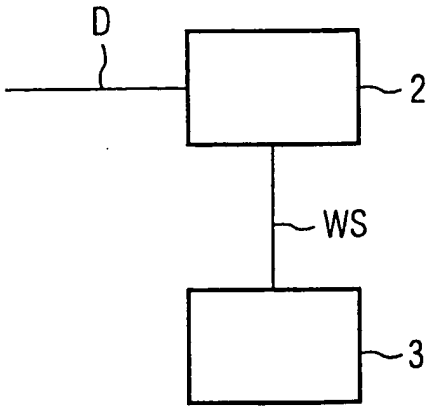


FIG 3



INTERNATIONAL SEARCH REPORT

Internal Application No
PCT/DE 99/01461

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G06F G07F G11C G06K

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 4 932 053 A (FRUHAUF SERGE ET AL) 5 June 1990 (1990-06-05) column 2, line 29 -column 3, line 5	1,2
X	EP 0 790 547 A (SGS THOMSON MICROELECTRONICS) 20 August 1997 (1997-08-20) column 1, line 45 -column 2, line 14	1,2
X	US 5 404 402 A (SPRUNK ERIC) 4 April 1995 (1995-04-04) column 2, line 5 -column 3, line 9	1,2
A	US 5 533 123 A (NORCROSS THOMAS M ET AL) 2 July 1996 (1996-07-02) column 16, line 13-47	1-6

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 October 1999	28/10/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Nygren, P

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Intern ·al Application No
PCT/DE 99/01461

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	DE 195 23 466 C (INFORMATIKZENTRUM DER SPARKASS) 3 April 1997 (1997-04-03) the whole document	1-6

1

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

...ormation on patent family members

Internat al Application No
PCT/DE 99/01461

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 4932053 A	05-06-1990	FR 2638869 A	11-05-1990
		EP 0368727 A	16-05-1990
		JP 2199561 A	07-08-1990
		JP 2813663 B	22-10-1998
EP 0790547 A	20-08-1997	FR 2745099 A	22-08-1997
		JP 9230957 A	05-09-1997
US 5404402 A	04-04-1995	EP 0660562 A	28-06-1995
		JP 7239837 A	12-09-1995
		NO 944432 A	22-06-1995
US 5533123 A	02-07-1996	EP 0715733 A	12-06-1996
		WO 9600953 A	11-01-1996
DE 19523466 C	03-04-1997	NONE	

INTERNATIONALER RECHERCHENBERICHT

Interna ales Aktenzeichen
PCT/DE 99/01461

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 6 G06F1/00

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 6 G06F G07F G11C G06K

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 4 932 053 A (FRUHAUF SERGE ET AL) 5. Juni 1990 (1990-06-05) Spalte 2, Zeile 29 -Spalte 3, Zeile 5 ---	1,2
X	EP 0 790 547 A (SGS THOMSON MICROELECTRONICS) 20. August 1997 (1997-08-20) Spalte 1, Zeile 45 -Spalte 2, Zeile 14 ---	1,2
X	US 5 404 402 A (SPRUNK ERIC) 4. April 1995 (1995-04-04) Spalte 2, Zeile 5 -Spalte 3, Zeile 9 ---	1,2
A	US 5 533 123 A (NORCROSS THOMAS M ET AL) 2. Juli 1996 (1996-07-02) Spalte 16, Zeile 13-47 --- -/--	1-6

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der Internationalen Recherche	Absendedatum des internationalen Recherchenberichts
20. Oktober 1999	28/10/1999

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Nygren, P

1

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Intern ales Aktenzeichen
PCT/DE 99/01461

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	DE 195 23 466 C (INFORMATIKZENTRUM DER SPARKASS) 3. April 1997 (1997-04-03) das ganze Dokument	1-6

1

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Interne ...les Aktenzeichen
PCT/DE 99/01461

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 4932053 A	05-06-1990	FR 2638869 A	11-05-1990
		EP 0368727 A	16-05-1990
		JP 2199561 A	07-08-1990
		JP 2813663 B	22-10-1998
EP 0790547 A	20-08-1997	FR 2745099 A	22-08-1997
		JP 9230957 A	05-09-1997
US 5404402 A	04-04-1995	EP 0660562 A	28-06-1995
		JP 7239837 A	12-09-1995
		NO 944432 A	22-06-1995
US 5533123 A	02-07-1996	EP 0715733 A	12-06-1996
		WO 9600953 A	11-01-1996
DE 19523466 C	03-04-1997	KEINE	